PROCESSING ACTIVITY MASKING IN A DATA PROCESSING SYSTEM

This invention relates to the field of data processing systems. More particularly, this invention relates to the masking of processing activity within data processing systems, for example, in order to increase security.

It is known to provide data processing systems which manipulate secure data and for which it is desirable to ensure a high degree of security. As an example, it is known to provide smart cards which include a data processing system which manipulates secure data, such as secret cryptographic keys, and this data must be kept secret in order to prevent fraud.

Known ways of attacking the security of such systems include timing analysis and power analysis. By observing the timing behaviour and/or the power consumption behaviour of such a system in response to inputs, information concerning the processing being performed and the data being manipulated can be determined in a way that can compromise security. It is strongly advantageous to provide resistance against such security attacks.

Viewed from one aspect the present invention provides apparatus for processing data, said apparatus comprising:

a data processing register operable to store a data value;

a register writing circuit operable to store a data value to said data processing register; and

three or more further registers; wherein

when said register write circuit writes a data value to said data processing register, said register write circuit also writes data values to three or more further registers such that a fixed relative number of bits within said data processing register and said three or more further registers as a whole transition from high to low and from low to high irrespective of what data value is being written to said data processing register and what data value was previously stored within said data processing register.

This invention recognises that when a register write occurs there can be a difference in the power consumed and/or other characteristics depending upon how many bit values transition from high to low compared with how many bit values transition from low to high. The invention overcomes this problem by providing three or more further registers to which appropriate data values are written at the same time. such that the number of high to low transitions and low to high transitions does not

change irrespective of what data value is being written and what the previous data value was. This enhances security by masking potentially externally visible characteristics having a dependence upon data values being processed. The technique is also applicable to systems in which multiple writes occur in parallel to multiple registers, e.g. a superscalar processor.

Whilst it is possible that a variety of different mathematical relationships may be determined between the true data value being written and the data values written in the three or more further registers that will satisfy the non - varying requirement, particularly preferred embodiments of the invention which are advantageously simple are such that said register writing circuit writes a value X_i to an i^{th} bit of said data processing register previously storing a value of Y_i, said register writing circuit also writes to corresponding bit positions within three further registers respective values of:

an inverse of X_i;

a new value Rd_i given by (inverse (X_i XOR Y_i)) XOR (a value of Rd_i currently stored)); and

an inverse said new value of Rd_i.

This particular relationship balances the transitions and yet is relatively simple to calculate and uses relatively few further registers in a manner which is advantageous from a circuit requirement and power consumption point of view.

Whilst the present invention could be used to protect against the leakage of information due to writes from a single data register, the invention is well suited to embodiments in which a register bank of a plurality of data registers is provided.

Within such an environment dedicated dummy registers may be provided in combination with some shared dummy registers. The sharing of some of the dummy registers enables the circuit resources needed for this techniques to be advantageously reduced whilst still allowing a guaranteed balance in the number of transitions from high to low and low to high.

It is convenient to provide embodiments to which the dedicated dummy register stores the inverse of the value held within the real data register and the shared dummy registers store the exclusive OR of the new data value with the old data value as well as the inverse of this exclusive OR.

Whilst this technique may be utilised for all of the registers within a register bank, it is often the case that some registers within the register bank have dedicated

non-secure roles, such as program counter, stack pointer, return address and the like, which mean that the balance between the additional circuit resources required against the security issue is such that it is preferred not to utilise this technique in association with those registers.

Viewed from another aspect the present invention provides a method of processing data, said method comprising the steps of:

storing a data value in a data processing register; and

when said data value is stored in said data processing register also storing data values within three or more further registers such than a fixed relative number of bits within said data processing register and said three or more further registers as a whole transition from high to low and from low to high irrespective of what said data value is being written to data processing register and what data value was previously stored within said data processing register.

Embodiments of the invention will now be described, by way of example only, with reference to the accompanying drawings in which:

Figure 1 schematically illustrates a data processing system operable in a fixed timing mode and a variable timing mode;

Figure 2 schematically illustrates a conditional programming instruction;

Figure 3 is a flow diagram schematically illustrating part of the processing operations performed by an instruction decoder operating in accordance with the present techniques;

Figure 4 schematically illustrates the execution of a conditional branch instruction in a fixed timing mode;

Figure 5 is a diagram schematically illustrating a data processing system including multiple circuit portions which may be selectively enabled to perform required processing operations or dummy processing operations;

Figure 6 schematically illustrates a circuit portion and its associated dummy activity enabling circuit which may be responsive to both required enable signals and random dummy activity enable signals;

Figure 7 schematically illustrates a linear shift back feed register which may be used as a pseudo-random signal generator:

Figure 8 is a flow diagram schematically illustrating control of a circuit portion to perform required processing activity and dummy processing activity;

Figure 9 schematically illustrates a portion of a register bank including multiple data processing registers, multiple dummy registers, multiple shared dummy